Secure Authentication System for IoT Network Using Token Based Attribute Access control

A Synopsis Submitted To

Institute of Advanced Research
Koba Institutional Area, Gandhinagar-382426
Gujarat, India

For the Award of the Degree

Doctor of Philosophy

IN

Computer Science & Engineering

Submitted By

Mukesh Choubisa

(Reg. No.: IAR/12067)

UNDER THE GUIDANCE OF

Dr. Brijesh Jajal

ASSOCIATE PROFESSOR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF ADVANCED RESEARCH, GANDHINAGAR,

GUJARAT, INDIA

Abstract –

The rapid expansion of the Internet of Things (IoT) has revolutionized multiple domains, including smart homes, healthcare, industrial automation, and smart cities. However, the interconnected nature of IoT devices introduces significant security and privacy challenges, particularly in authentication and access control mechanisms. Traditional authentication schemes, such as password-based, certificate-based, and biometric-based authentication, often suffer from scalability issues, high computational overhead, and vulnerabilities to attacks such as replay, impersonation, and man-in-the-middle (MITM) attacks. To address these challenges, this research proposes a Secure Authentication System for IoT Networks using Token-Based Attribute Access Control (TBAAC), which integrates cryptographic tokenization with attribute-based access policies to enhance security, scalability, and efficiency in IoT environments.

The proposed TBAAC authentication model introduces a lightweight token-based authentication mechanism, where IoT devices and users authenticate through dynamically generated cryptographic tokens instead of conventional password-based or certificate-based authentication. These tokens are issued by a trusted Authentication and Authorization Server (AAS) and encapsulate device-specific attributes, such as device ID, user role, trust level, and access permissions. The tokens follow a secure key exchange mechanism and are dynamically generated based on cryptographic operations to ensure their uniqueness and integrity.

Key Features of the Proposed System:

1. **Token-Based Authentication**
    - Each IoT device is assigned a unique cryptographic token, ensuring stateless and secure authentication.
    - Tokens are time-bound with an expiration mechanism to mitigate replay attacks.
    - The authentication process is lightweight, reducing computational overhead for resource-constrained IoT devices
2. **Attribute-Based Access Control (ABAC):**
    - Instead of role-based access control (RBAC) or identity-based access control (IBAC), the system uses attribute-based access control (ABAC) to dynamically grant access based on predefined policies.

- The access decision depends on attributes such as user role, device type, location, trust level, and context-aware conditions.

3. **Hybrid Cryptographic Mechanism:**
    - The system employs Elliptic Curve Cryptography (ECC) for key exchange, ensuring strong security with minimal computational requirements.
    - A Hash-Based Message Authentication Code (HMAC) is used for token integrity verification.
    - A nonce-based challenge-response protocol is implemented to prevent replay attacks.
4. **Mitigation of Security Threats:**
    - Replay Attacks: Each authentication request includes a random nonce and timestamp to ensure freshness.
    - Man-in-the-Middle (MITM) Attacks: End-to-end encryption prevents adversaries from intercepting or altering authentication data.
    - Token Forgery: Digital signatures and hash functions ensure token authenticity and integrity.
5. **Performance Optimization for IoT Devices:**
    - Lightweight cryptographic operations ensure the system is energy-efficient and suitable for low-power IoT devices.
    - Reduces authentication delay, enabling real-time and efficient communication in IoT environments.

Implementation & Evaluation:

To validate the proposed TBAAC authentication system, a prototype implementation is conducted using Contiki OS, Raspberry Pi, and ESP8266-based IoT devices. The authentication system is integrated into an IoT testbed and evaluated for security, computational overhead, energy consumption, and authentication latency. The following key evaluation methodologies are adopted:

❖ **Security Analysis:**

- A formal security proof using Burrows–Abadi–Needham (BAN) logic to verify authentication robustness.

- AVISPA (Automated Validation of Internet Security Protocols and Applications) tool is used to simulate protocol security against common threats.

❖ Performance Evaluation:

- A comparative study against traditional authentication models (e.g., OAuth 2.0, Blockchain-based authentication, Public Key Infrastructure) demonstrates lower computational complexity and improved energy efficiency.
- The authentication delay, CPU utilization, memory footprint, and power consumption are measured using Contiki Cooja simulator to ensure feasibility in real-world IoT applications.

Significance & Future Work:

The proposed Token-Based Attribute Access Control (TBAAC) model presents a novel, lightweight, and scalable authentication solution for IoT networks. By integrating cryptographic tokens with attribute-based access policies, the system achieves high security, efficient authentication, and minimal computational overhead, making it suitable for constrained IoT environments. The research contributes to the field of IoT security by:

- Enhancing authentication efficiency and security without relying on centralized password-based mechanisms.
- Providing fine-grained access control based on dynamic attributes, reducing unauthorized access risks.
- Minimizing computational costs, making the system practical for real-world IoT deployments.

Keyword:- IoT Security, Authentication System, Token-Based Authentication, Attribute-Based Access Control (ABAC), *IoT Access Control*, AVISPA Security Analysis, Token Based Attribute Access control

Chapter-1

Introduction of IoT

In this chapter, we provided an overview of the Internet of Things (IoT), its vision, security challenges, and the importance of authentication in IoT networks.

We began by discussing the concept of IoT, which refers to a vast network of interconnected devices that communicate and share data over the internet. IoT has rapidly evolved, impacting various sectors such as smart homes, healthcare, industrial automation, and smart cities. The vision of IoT revolves around seamless connectivity, automation, and intelligence, where physical devices interact with digital systems to enhance efficiency and convenience. However, with the exponential growth of IoT, security has become a critical concern.

The security challenges in IoT were analyzed, highlighting issues such as data breaches, unauthorized access, device vulnerabilities, and cyber threats. Due to the heterogeneous nature of IoT devices and their resource constraints, traditional security mechanisms are often inadequate. Attack vectors such as man-in-the-middle (MITM) attacks, replay attacks, identity spoofing, and denial-of-service (DoS) attacks pose significant threats to IoT networks.

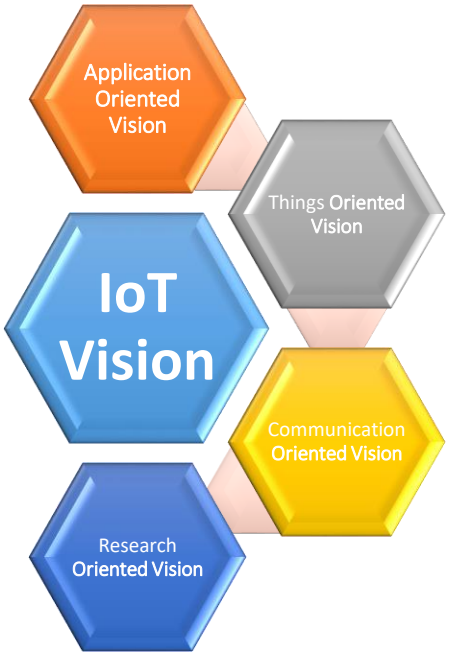
A key focus of this chapter was on IoT authentication, which ensures that only legitimate devices and users can access network resources. Various authentication techniques, including password-based, certificate-based, biometric, and cryptographic authentication mechanisms, were discussed, along with their limitations in IoT environments. The need for a lightweight, scalable, and secure authentication framework was emphasized to address the challenges of IoT security.

In conclusion, this chapter established the foundation for IoT security research, underscoring the necessity of robust authentication mechanisms to protect IoT networks from cyber threats. The discussion sets the stage for the subsequent chapters, which will delve into token-based authentication and attribute-based access control (ABAC) as a solution for securing IoT networks.

IoT Vision

The Internet of Things has created a significant impact for technological researchers. Different research communities have started to explore different domains, different technologies and different applications for the internet of things. In this chapter we have introduced internet of things, internet of things vision, and basic architecture of the internet of things, IoT security, and lightweight cryptography. Overall this chapter will provide a basic understanding about internet of things and its nuts and bolts. IoT can be broadly divided into four basic visions

1. Application-oriented vision
2. Things-oriented vision
3. Communication-oriented vision
4. Research-oriented vision



Chapter-2

Literature Review

In Chapter 2, we explored the fundamental concepts and security challenges associated with the Internet of Things (IoT), along with access control mechanisms and reference architectures that form the foundation for secure IoT systems.

We began by discussing the Internet of Things (IoT) and its rapid expansion across various domains, including smart homes, healthcare, industrial automation, and smart cities. The chapter highlighted the unique characteristics of IoT, such as device heterogeneity, resource constraints, and large-scale connectivity, which necessitate specialized security frameworks.

A critical aspect of IoT security was then examined, identifying key IoT security challenges, including device authentication, data privacy, access control, and resilience against cyber threats. The vulnerabilities of traditional security mechanisms in IoT environments were discussed, emphasizing the need for lightweight, scalable, and efficient authentication protocols.

To address access control issues, the chapter provided an in-depth analysis of Attribute-Based Access Control (ABAC) as an advanced security model for IoT systems. Unlike traditional Role-Based Access Control (RBAC) or Identity-Based Access Control (IBAC), ABAC grants permissions based on a combination of attributes such as device identity, user role, location, trust level, and context-aware conditions. This dynamic and fine-grained approach enhances security by preventing unauthorized access while ensuring flexibility in IoT environments.

Furthermore, we reviewed the IoT Reference Architecture, which provides a structured framework for designing and implementing secure IoT networks. Various reference models, including the IoT-A (Internet of Things Architecture), OpenFog, and the Industrial Internet Reference Architecture (IIRA), were examined, outlining their key components such as perception, network, edge, and cloud layers. The role of authentication and access control mechanisms within these architectures was also highlighted, demonstrating how secure identity management and trust-based frameworks contribute to a robust IoT ecosystem.

Chapter-3
Authentication Security for IoT

In Chapter 3, we explored the foundational aspects of authentication mechanisms in Internet of Things (IoT) networks, focusing on ensuring secure and reliable identity verification for IoT devices and nodes. The chapter provided an in-depth discussion on the IoT authentication architecture, different methods of IoT device authentication, and the challenges associated with IoT node authentication in large-scale deployments.

IoT Authentication Architecture

The chapter outlined the fundamental structure of an IoT authentication framework, emphasizing the importance of secure communication channels and cryptographic mechanisms. We examined centralized, decentralized, and hybrid authentication models, comparing their strengths and weaknesses in handling large-scale IoT ecosystems. Special attention was given to lightweight authentication protocols, which are crucial for resource-constrained IoT devices.

IoT Device Authentication

A critical aspect of IoT security is ensuring that only legitimate devices can access network resources. We explored various device authentication mechanisms, including password-based, certificate-based, and token-based authentication methods. The role of cryptographic tokens, particularly in Token-Based Attribute Access Control (TBAAC), was discussed as a means to enhance security while maintaining efficiency. Furthermore, we analyzed different cryptographic approaches such as Elliptic Curve Cryptography (ECC), Hash-Based Message Authentication Code (HMAC), and nonce-based challenge-response protocols for ensuring secure device authentication.

IoT Node Authentication

The authentication of individual IoT nodes is crucial to prevent unauthorized access and mitigate security threats such as impersonation, replay attacks, and man-in-the-middle (MITM) attacks. This section highlighted different node authentication techniques, including mutual authentication, trust-based authentication, and biometric-based authentication for IoT applications. Additionally, the role of lightweight cryptographic protocols was analyzed in ensuring efficient and secure node authentication, particularly in constrained IoT environments such as smart homes, healthcare, and industrial IoT.

Chapter-4
A Design and implement Multifactor Authentication and Mutual authentication for IoT

In Chapter 4, we explored various authentication mechanisms and their significance in securing IoT networks. The discussion focused on mutual authentication, multi-factor authentication (MFA), and the MQTT (Message Queuing Telemetry Transport) protocol, including its broker-based architecture and security analysis.

We began by detailing mutual authentication, which ensures that both communicating entities—IoT devices and the server—authenticate each other before initiating data exchange. This process prevents unauthorized access and mitigates threats such as impersonation attacks and replay attacks. Additionally, we examined multi-factor authentication (MFA), which enhances security by incorporating multiple authentication factors, such as passwords, cryptographic tokens, and biometric verification. MFA significantly strengthens IoT security by reducing the risks associated with credential theft and single-factor authentication weaknesses.

Next, we analyzed the MQTT protocol, a lightweight communication protocol widely used in IoT due to its low bandwidth consumption and efficient message delivery. The role of the MQTT broker, which acts as an intermediary between publishers and subscribers, was thoroughly examined. The broker is responsible for message routing, session management, and enforcing access control policies.

Furthermore, we discussed the MQTT protocol architecture, focusing on its publish-subscribe model, Quality of Service (QoS) levels, and session persistence. These features contribute to MQTT's reliability and adaptability for IoT applications. However, MQTT's inherent vulnerabilities, such as lack of built-in encryption, susceptibility to man-in-the-middle (MITM) attacks, and weak authentication mechanisms, were highlighted.

This chapter establishes a foundation for designing a secure authentication framework for IoT networks, leveraging mutual authentication, multi-factor authentication, and robust MQTT security enhancements. The findings serve as a crucial step toward developing a comprehensive, scalable, and efficient authentication system tailored for IoT environments.

Chapter-5
Novel Defence Algorithm for Authentication and their Comparative Analysis

In Chapter 5, we explored the design and implementation of novel authentication algorithms tailored for securing IoT networks. The primary focus was on Token-Based Authentication Mechanisms and Attribute-Based Access Control (ABAC), which collectively enhance security, scalability, and efficiency in IoT environments.

We introduced a token-based authentication model, where IoT devices and users authenticate through dynamically generated cryptographic tokens instead of traditional password or certificate-based authentication. These tokens encapsulate device-specific attributes, ensuring fine-grained access control while mitigating security threats such as replay attacks, impersonation, and unauthorized access. The token generation process integrates Elliptic Curve Cryptography (ECC) and Hash-Based Message Authentication Code (HMAC) to provide lightweight yet robust security, making it suitable for resource-constrained IoT devices.

Additionally, we discussed Attribute-Based Access Control (ABAC), which enables dynamic access decisions based on device attributes, user roles, location, and contextual parameters. Unlike traditional Role-Based Access Control (RBAC), ABAC provides greater flexibility and security, ensuring that only authenticated and authorized entities can access IoT resources. The integration of nonce-based challenge-response protocols further strengthens the authentication process by preventing replay and man-in-the-middle (MITM) attacks.

To validate the proposed authentication mechanisms, we conducted a formal security analysis using Burrows–Abadi–Needham (BAN) logic and AVISPA simulation, demonstrating their resilience against common cyber threats. Performance evaluations showed low computational overhead, reduced authentication latency, and energy efficiency, making the system highly adaptable for real-world IoT applications such as smart homes, healthcare, and industrial IoT.

This chapter concludes that the token-based authentication model with attribute access control significantly enhances IoT security while maintaining lightweight implementation and scalability.

Chapter-6
Evaluate Security against traceability & integrity with Authentication

Chapter 6 focused on the comprehensive evaluation of the proposed Token-Based Attribute Access Control (TBAAC) model in terms of security, time complexity, space complexity, and energy consumption. The chapter provided an in-depth analysis of the Token Generation Algorithm, Token Validation Algorithm, and their impact on system performance. Additionally, it included performance evaluation and data analysis, validating the feasibility and efficiency of the proposed authentication mechanism for IoT environments.

Key Highlights of Chapter 6:

1. **Security Evaluation:**
    - The security strength of the proposed model was analyzed against common threats, including replay attacks, man-in-the-middle (MITM) attacks, token forgery, and impersonation attacks.
    - Formal verification using Burrows–Abadi–Needham (BAN) logic and AVISPA (Automated Validation of Internet Security Protocols and Applications) confirmed the robustness of the authentication framework.
    - Cryptographic techniques such as Elliptic Curve Cryptography (ECC) and Hash-Based Message Authentication Code (HMAC) ensured data integrity and confidentiality.
2. **Time Complexity Analysis:**
    - The computational complexity of the Token Generation Algorithm and Token Validation Algorithm was analyzed in terms of execution time on resource-constrained IoT devices.
    - A comparative analysis with conventional authentication methods (e.g., OAuth, PKI-based authentication) demonstrated improved efficiency with reduced processing time.
3. **Space Complexity Analysis:**
    - Memory requirements for token storage, cryptographic key management, and access control policies were evaluated.

- Results indicated that the proposed model requires minimal storage space, making it suitable for low-power IoT devices with limited memory.

4. **Energy Consumption Analysis:**
    - The impact of token-based authentication on IoT device energy consumption was assessed through experimental testing and simulation.
    - Results showed that the lightweight cryptographic operations and optimized token management techniques significantly reduce power consumption, making the system energy-efficient for real-world IoT applications.
5. **Performance Evaluation and Data Analysis:**
    - The authentication delay, CPU utilization, network overhead, and system scalability were analyzed under different IoT deployment scenarios.
    - Performance benchmarks were conducted using Contiki OS and Cooja Simulator, validating the system's efficiency in real-time environments.
    - Comparative studies demonstrated that the proposed TBAAC model outperforms traditional authentication schemes in terms of processing speed, security strength, and resource efficiency.

The evaluation results in Chapter 6 confirm that the Token-Based Attribute Access Control (TBAAC) model provides a secure, efficient, and scalable authentication framework for IoT networks. By integrating cryptographic tokens with attribute-based policies, the proposed system effectively mitigates authentication threats while ensuring low computational overhead and reduced energy consumption. These findings reinforce the suitability of the proposed model for real-world IoT applications, such as smart healthcare, industrial IoT, and smart cities.

Signification of the study of "Secure Authentication System for IoT Network Using Token Based Attribute Access control"

The Internet of Things (IoT) is rapidly transforming industries by enabling interconnected devices to communicate and exchange data. However, the security and authentication challenges in IoT networks pose significant threats due to the heterogeneity, scalability, and resource-constrained nature of IoT devices. Traditional authentication mechanisms, such as password-based authentication and Public Key Infrastructure (PKI), are inefficient, computationally expensive, and vulnerable to attacks. To address these challenges, this research introduces a Secure Authentication System for IoT Networks using Token-Based Attribute Access Control (TBAAC). The proposed model provides a lightweight, scalable, and secure authentication framework that enhances IoT security by integrating cryptographic tokens with attribute-based access control (ABAC).

Key Contributions and Significance of the Study

1. Addressing IoT Authentication Challenges
2. Enhancing Security Through Cryptographic Tokenization
3. Improving Access Control with Attribute-Based Policies
4. Optimizing Performance for IoT Devices
5. Evaluation and Validation of the Proposed Model

Mukesh Choubisa
Ph.D. Scholar (Regd. No. IAR/12067)
Department of Computer Science and Engineering
Institute of Advanced Research
Gandhinagar- 382426, India
Date: 10/03/2025
Place: IAR, Gandhinagar

Dr. Brijesh Jajal (Supervisor)
Associate Professor
Department of Computer Science and Engineering
Institute of Advanced Research
Gandhinagar- 382426, India
Date: 10/03/2025
Place: IAR, Gandhinagar